Cyber@UC Meeting 81

Intel Management Engine and Other Coprocessors

If You're New!

- Join our Slack: cyberatuc.slack.com
- Check out our website: cyberatuc.org
- **SIGN IN!** (Slackbot will post the link in #general every Wed@6:30)
- Feel free to get involved with one of our committees: *Content Finance Public Affairs Outreach Recruitment Lab*
- Ongoing work in our research lab!



Announcements

- Looking for **lab committee** volunteers!
- Merchandise on the way, Online Shop
- STEM FEST on Dec 1st!
- We're going to NorseRage's CTF at NKU on November 28th (**tomorrow**)
- The TVs are **finally** mounted!
- Ohio Officials visited our RAPIDS Lab!
- Battelle Internships





Weekly News

Over the Winter Break:

- Marriott Hotel chain data breach exposes 500 million passport numbers
- Donald Trump gets the top government shutdown streak in US history
- U. S. Military expresses interest in securing supply chains against attacks as well as preventing cyber espionage in the private sector, currently unknown if this will manifest as another duty of the US Cyber Command or something else
- Pwn2Own hacking conference will be featuring a Tesla Model 3 this year, goal of PWn2Own is to successfully demonstrate an exploit of a target device then reveal that exploit to the vendor in exchange for the exploited product

Sources

https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-2 02/2019/01/08/the-cybersecurity-202-how-one-key-democrat-plans-to-watchd og-offensive-hacking-operations/5c338eba1b326b66fc5a1bc8/?noredirect=on& utm_term=.7ce98e45f404

https://jalopnik.com/if-you-can-hack-into-this-tesla-model-3-its-yours-1831746 885



Intel Management Engine and Other Coprocessors

Processors inside processors

Previous Work / Recommended Content

DEF CON 26: Christopher Domas - GOD MODE UNLOCKED Hardware Backdoors in redacted x86

DEF CON 26 - Christopher Domas - The Ring 0 Facade Awakening the Processors Inner Demons

Christopher Domas's Github at https://github.com/xoreaxeaxeax



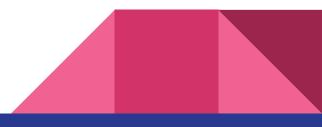
What is/are IME and Coprocessors

- Intel Management Engine (IME)/Active Management Technology (AMT) and similar products from other vendors (Coprocessors / CP's)
- Originally meant for streamlining IT work on servers and desktops (similar to how we are using iDRAC to configure our lab servers over the network)
- Physically separate processor embedded within the x86 processor that runs a custom MINIX image
- Basically allow vendors to sell products that can be configured over the network in very interesting and proprietary ways



Evolution of IME and Coprocessors (CP)

- Early versions started with basic network configuration and firmware update functions
- Later versions added more complex network support (wireless and IPv6) as well as additional cryptographic features and protections to try and prevent end user access to the IME/CP
- Current versions of the IME have full OS-independent access to the systems running on the processors as well as very aggressive self-health monitoring to make sure that only the original Intel signed firmware is on the device



Implications of IME and CP's

- Basically a vendor-only backdoor into the processor on a system
- Has complete root access to the systems at all times
- Powered on even when the main computer is shut-off (computer must be disconnected from power to shutdown the IME)
- No public auditing (security through obscurity) or functionality documentation (NDA's required for even basic documentation)
- Even Google, the largest software company in the world, has struggled to move past the blackbox of the IME in their attempt to remove closed-source and third party software from their systems

Concerns that IME/Coprocessors are Gov. Tools

Hazardous Locations Certification	 Hazardous Locations Certification, 4 in 1 	\$0.00
	No Hazardous Locations Certification	Included in price
Systems Management	No Out-of-Band Systems Management	Included in price
	O Intel vPro [™] - ME Inoperable, Custom Order	+ \$20.97
	O Intel vPro™ Technology's Advanced Management Features	+ \$20.97
Memory ⁱ	Help Me Choose	
	4GB (1x4GB) 2133MHz DDR4 Memory	Included in price
	8GB (1x8GB) 2133MHz DDR4 Memory	+ \$76.88

Other Stuff

- <u>https://en.wikipedia.org/wiki/Intel_AMT_versions</u>
- <u>https://github.com/xoreaxeaxeax</u>





https://en.wikipedia.org/wiki/Intel_AMT_versions https://www.tomshardware.com/news/google-removing-minix-management-engi ne-intel,35876.html https://libreboot.org/fag.html#intelme

